



Docket No.: P2001,0154

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313 20231.

By:

Date: October 1, 2003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applic. No. : 10/661,341  
Applicant : Bernd Meyer, Erwin Hess  
Filed : September 12, 2003  
Art Unit : to be assigned  
Examiner : to be assigned

Docket No. : P2001,0154  
Customer No.: 24131

CLAIM FOR PRIORITY

Hon. Commissioner for Patents,  
Alexandria, VA 22313-1450

Sir:

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119, based upon the German Patent Application 101 11 756.6 filed March 12, 2001.

A certified copy of the above-mentioned foreign patent application is being submitted herewith.

Respectfully submitted,

GREGORY L. MAYBACK  
REG. NO. 40,716

Date: October 1, 2003

Lerner and Greenberg, P.A.  
Post Office Box 2480  
Hollywood, FL 33022-2480  
Tel: (954) 925-1100  
Fax: (954) 925-1101

/mjb

# BUNDESREPUBLIK DEUTSCHLAND



## Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 101 11 756.6

Anmeldetag: 12. März 2001

Anmelder/Inhaber: Infineon Technologies AG,  
München/DE

Bezeichnung: Verfahren zur Authentikation

IPC: H 04 L, G 06 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 11. September 2003  
Deutsches Patent- und Markenamt  
Der Präsident  
Im Auftrag

A handwritten signature in black ink, appearing to read "Schweiger".

Beschreibung

Verfahren zur Authentikation

- 5 Die vorliegende Erfindung betrifft ein Verfahren zur Authen-  
tikation eines Datensatzes zwischen einer beweisführenden  
Einheit und einer verifizierenden Einheit in der Datenverar-  
beitung.
- 10 Im Bereich der Verwendung von Chipkarten als Kredit-, Debit-,  
Geld-, Identifikations-, Zugangs- oder Zeitkontrollkarten  
etc. oder etwa als Nachrichtenträger stellt die Frage des  
Schutzes der auf der Karte vorhandenen Informationen vor ei-  
nem unberechtigten Zugriff Dritter ein zentrales Problem dar.
- 15 Ein besonderer Aspekt ist dabei auch die gesicherte Daten-  
übertragung zwischen der Chipkarte und z.B. dem CAD (card ad-  
apter device) eines Chipkartenterminals. Dies wird durch den  
Prozeß der sog. Authentikation der beteiligten Einheiten,  
hier der Chipkarte und dem Terminal, ermöglicht: dabei ge-  
langt z.B. das Terminal zu dem hinreichend gesicherten Nach-  
weis über die Identität der mit ihm in einem Protokoll  
befindlichen Chipkarte. Im Gegenzug kann durch einen entspre-  
chenden Prozeß auch die Chipkarte Sicherheit über die Identi-  
tät des Terminals im Moment der gegenseitigen Überprüfung  
25 erlangen. Entsprechendes gilt auch für die Authentizität der  
übertragenen Daten.

Der Nachweis der Identität kann dadurch geliefert werden, daß  
nur den beteiligten Einheiten bekannte, geheime Informationen  
30 ausgetauscht werden. Man unterscheidet hierbei die sog.  
schwache und starke Authentikation. Bei der erstgenannten

gibt z.B. der Besitzer einer Magnetstreifenkarte ein Paßwort oder eine PIN über eine Tastatur ein und authentifiziert sich somit als rechtmäßiger Eigentümer seiner Karte. Hierbei wird das Geheimnis übertragen. Bei der starken Authentikation

5 tauscht in einem sog. Challenge-Response-Verfahren eine die Identität des Protokollpartners verifizierende Einheit (im folgenden engl. verifier genannt) in einem Dialog mit der über ihre Identität beweisführenden Einheit (im folgenden engl. prover genannt) Authentisierungsinformation aus, die

10 das Vorhandensein eines Geheimnisses belegt, ohne dies aber einem Angreifer preiszugeben. Das Protokollverfahren zwischen den Einheiten ist dabei meist a priori festgelegt.

Werden nach oder anstatt Informationen über die Identität der 15 beteiligten Einheiten nur Daten transferiert, welche einem ähnlich hohen Sicherheitsbedürfnis unterliegen, so kann unter Anwendung eines analogen Protokollverfahrens auch verallgemeinert von einer Datenauthentikation gesprochen werden. Ein bekanntes Beispiel hierzu sind etwa die noch vorhandenen 20 Geldbeträge auf Telefonkarten, welche dem Telefonterminal von der Karte authentisch mitgeteilt werden.

Bei der für Chipkarten besonders wichtigen starken Authentikation haben sich im wesentlichen zwei Ansätze für verschiedene Anwendungen herauskristallisiert. Vom Einsatz bei Telefonkarten (Geldkarten) her bekannt ist die Verwendung von 25 symmetrischen Authentikationsverfahren zum Austausch von Identitätskennzeichen und Daten. Das Grundprinzip besteht darin, daß für die Authentikation der Karte (des Provers) gegenüber dem Terminal (dem Verifier) dieses zunächst der Karte 30 eine Zufallszahl sendet, welche aus dieser Zufallszahl mit

einem beiden Einheiten bekannten Geheimschlüssel unter Verwendung eines geeigneten Verfahrens einen Authentikationswert errechnet und anschließend dem Terminal zurücksendet. Dieses erkennt durch Vergleich der mit seinem Schlüssel durchgeführten Berechnungen mit der ursprünglich gesendeten Zufallszahl, ob die Karte den autorisierten Schlüssel verwendet hat. Der Karten- und Terminalhersteller verwendet hierzu oft das sog. Masterkey-Konzept, bei dem in jedem Terminal dieser Masterkey hinterlegt ist, aus welchem sich der bei der Kartencodierung (engl. card personalization) der Karte zugeordnete individuelle Schlüssel mittels eines Algorithmus aus ihrer Identitätskennzahl berechnen lässt. Ein älterer, bekannter Standard hierzu ist der data encryption standard (DES).

Gelingt es einem Angreifer in den Besitz des Masterkeys zu gelangen, so entsteht das Problem, daß das gesamte System für diesen offengelegt ist. Dieser Nachteil könnte durch Verwendung individuell für jede Karte hinterlegter Schlüsselpaare umgangen werden, welches jedoch beispielsweise durch die hohe Zahl im Umlauf befindlicher Telefonkarten und damit Schlüssel unpraktikabel ist. Im Falle von Telefonkarten behilft man sich heute umständlich mit weiteren kryptographischen Maßnahmen, welche auch einen Wechsel und eine eingeschränkte Gültigkeit der Masterkeys beinhalten.

Eine Alternative zu den symmetrischen Verfahren stellt das Versenden digitaler Signaturen in asymmetrischen Verfahren dar. Der Verifier (das Terminal) erzeugt eine Zufallszahl und sendet diese an den Prover (die Karte). Dieser signiert die Zufallszahl mit einem Verfahren zum Erzeugen digitaler Signaturen unter Verwendung eines nur ihm bekannten privaten

Schlüssels eines Schlüsselpaares - der öffentliche Schlüssel liegt sowohl dem Prover als auch insbesondere dem Verifier vor. An den Verifier zurückgesendet, wird die digitale Signatur mit dem öffentlichen Schlüssel auf ihre Korrektheit überprüft, wobei der Verifier nicht in Kenntnis des privaten Schlüssels gelangt, sondern nur die Information erhält, daß der Prover sich im Besitz des privaten Schlüssels befindet und damit authentifiziert ist. Ein häufig benutzter Algorithmus für diese Methode stammt von Rivest, Shamir und Adleman (RSA).

Leider ist bei diesen Verfahren unter Verwendung digitaler Signaturen ein hoher Rechenaufwand bedingt durch die Langzahl-Modulo-Arithmetik auf Seiten des Provers, also z.B. auf einer Chipkarte, notwendig. Typischerweise müssen dabei zwei sehr große Zahlen miteinander multipliziert und wieder modular reduziert (auf die Ursprungsgröße zurückgebracht) werden. Die Hardwareimplementierung auf dem Chip einer Chipkarte führt dadurch einerseits zu einer kostenaufwendigeren Chipkartenherstellung oder auch zu unannehmbar langen Rechen- und Antwortzeiten.

Es ist daher die Aufgabe der Erfindung die Kosten und den implementierungstechnischen Aufwand bei der Authentifikation von Daten, insbesondere auch bei der Identifikation der beteiligten Einheiten, zu senken.

Die Aufgabe wird erfindungsgemäß durch die Maßnahmen des Patentanspruches 1 gelöst.

Gemäß der vorliegenden Erfindung wird ein Dialog eingeführt, bei welchem eine beweisende Einheit einer verifizierenden Einheit unter Verwendung asymmetrischer kryptographischer Schlüssel die Authentizität der von ihr übermittelten Daten nachweist. Insbesondere kann sie dabei auch ihre eigene Identität nachweisen. Als Einheiten werden direkt miteinander in Kontakt tretende Module betrachtet, wobei ein beliebiger Übertragungsweg, z.B. elektronisch, lichtoptisch, akustisch etc. benutzt werden kann, und es sich bei den Modulen um integrierte Schaltungen enthaltende Systeme handelt, z.B. Chipkarten, Kartenterminals, Datenverarbeitungsanlagen wie Personal-Computer oder Server, etc.

Bei dem Verfahren wird ein Paar von öffentlichen und privaten Schlüsseln verwendet, wovon der private Schlüssel nur der beweisführenden Einheit, dem Prover, bekannt ist, während bei beiden Einheiten der zum privaten Schlüssel passende öffentliche Schlüssel hinterlegt ist, welches entweder durch eine vorab gesendete Nachricht bzw. eine Vorabinstallation oder durch eine Online-Verbindung zu einem zentralen Server auf Seiten der verifizierenden Einheit, dem Verifier, bewerkstelligt werden kann.

Ein wesentlicher Teilschritt des Verfahrens besteht darin, beiden beteiligten Einheiten, dem Prover und dem Verifier, den Datensatz, welcher authentifiziert werden soll, im Klartext bereitzustellen. Die Übertragung dazu kann verschlüsselt oder unverschlüsselt erfolgen. Bei der Datenauthentikation ist der Datensatz typischerweise zunächst beim Prover vorhanden, wobei dieser dann den Datensatz an den Verifier übermittelt.

telt, während bei der Einheitenauthentikation auch der Datensatz vom Verifier an den Prover übermittelt werden kann.

In den Schritten b) bis e), also im ersten Teil des Dialoges,  
5 wird dem Prover wenigstens ein Datenelement, welches im zweiten Teil des Dialoges als symmetrischer, nur den beiden Einheiten bekannter Schlüssel dient, vom Verifier in verschlüsselter Form zugestellt. Dies entspricht zunächst einem asymmetrischen Verfahren, denn der Prover benutzt seinen privaten  
10 Schlüssel, um das Datenelement zu entziffern. Zwar hat wie in einem herkömmlichen asymmetrischen Challenge-Response-Protokoll der Prover einen privaten Schlüssel, jedoch verwendet er ihn im Gegensatz dazu erfindungsgemäß nicht zur Bildung einer digitalen Signatur, sondern nur zur Entschlüsselung des empfangen, später selbst als Schlüssel dienenden wenigstens ei  
15 nen Datenelementes. Die Schritte b) bis e) folgen in ihrem zeitlichen Ablauf der im Anspruch angegebenen Reihenfolge.

Nach Schritt e) befinden sich die beiden Einheiten im Besitz  
20 des Klartextes des wenigstens einen Datenelementes. Der Austausch von mehr als nur einem Datenelement bietet sich an, wenn bei der Anwendung eines in den nachfolgenden Schritten vorgesehenen Algorithmus mehrfache Verknüpfungen des eigentlich zu authentisierenden Datensatzes mit den mehreren Datenelementen durchzuführen sind.

Die zur Erzeugung, Verschlüsselung, Übertragung und Entschlüsselung der mehreren Datenelemente jeweils notwendigen Sequenzen von Schritten können in beliebiger zeitlicher Zuordnung zueinander ausgeführt werden. Die relative zeitliche Zuordnung spielt also keine Rolle, es müssen aber alle Da  
30

tenelemente zu Beginn von Schritt f) beim Prover unverschlüsselt vorliegen.

In Schritt f) wird der zu authentisierende Datensatz unter  
5 Zuhilfenahme des wenigstens einen Datenelementes authenti-  
siert. Hierbei kann es sich wieder um ein asymmetrisches  
zweites kryptographisches Verfahren handeln, wenn nämlich das  
wenigstens eine Datenelement vom Verifier als öffentlicher  
Schlüssel zu einem weiteren, nur dem Verifier bekannten, pri-  
10 vaten Schlüssel erzeugt wurde. Vorzugsweise wird hier jedoch  
ein symmetrisches zweites kryptographisches Verfahren AUTGEN  
verwendet. Der vermittels AUTGEN in Abhängigkeit von dem we-  
nigstens einen Datenelement aus dem zu authentisierenden Da-  
tensatz gebildete - hier Authentikator genannte -  
15 transformierte Datensatz wird vom Prover wieder an den Veri-  
fier gesendet.

Der Verifier besitzt damit die Information über den Daten-  
satz, den symmetrischen Schlüssel, d.h. das von ihm selbst  
20 versendete, wenigstens eine Datenelement, den Authentikator  
sowie einen auf das Verfahren AUTGEN abgestimmten Authentika-  
tionsprüfalgorithmus. Dieses kann anhand des vorhandenen sym-  
metrischen Schlüssels den empfangenen Authentikator des  
Provers mit dem ursprünglichen Datensatz auf Korrektheit prü-  
25 fen.

Im letzten Schritt wertet der Verifier diesen Vergleich aus:  
gehören empfangener Authentikator und ursprünglicher Daten-  
satz zusammen, so gilt die Nachricht als vom Prover übermit-  
30 telt. Weitere Kommunikationsschritte können dann folgen. Bei

Nichtübereinstimmung kann der Verifier vorzugsweise die Kommunikation abbrechen.

- Bei diesem Verfahren entsteht ein großer Vorteil dadurch, daß
- 5 die im sicherheitstechnischen Sinn den symmetrischen Verfahren überlegenen Eigenschaften des Public-Key-Ansatzes, also der asymmetrischen Verfahren, ausgenutzt werden, ohne daß der bisher übliche implementierungstechnische Aufwand dabei anfällt, denn es ist beim erfindungsgemäßen Verfahren nicht
- 10 mehr erforderlich, eine rechenintensive Langzahl-Modulo-Arithmetik bereitzustellen. Ein besonders bei Chipkarten entstehender Vorteil ist, daß der private Schlüssel nur noch auf der Seite des Provers, hier also der Karte, dauerhaft gespeichert werden muß, ohne daß der Verifier im Laufe des Dialoges
- 15 in Kenntnis des Schlüssels kommt. Durch eine Implementierung mit aufeinander aufbauenden Rechenverfahren kann der auf dem Chip einer Chipkarte benötigte Platz für die Hardwareimplementierung erheblich verringert werden.
- 20 Nach einer weiteren Ausführungsform wird der Datensatz in Schritt a) vom Prover an den Verifier in unverschlüsselter Form, also als Klartext übermittelt. Dieser Schritt findet vor Schritt h) statt, "aus Zeitgründen idealerweise zusammen mit der Übersendung des Authentikators direkt vor oder nach
- 25 Schritt g). Diese Verfahrensform ist besonders günstig für die Datenauthentikation.

Nach einer weiteren Ausführungsform wird der Datensatz in Schritt a) vom Verifier als Zufallselement erzeugt und dem Prover übermittelt. Vorteilhaft ist es die Übermittlung asymmetrisch verschlüsselt durchzuführen, da dann einem potenti-

ellen Angreifer auch der Datensatz selber nicht zugänglich ist. Bei der verschlüsselten Übermittlung können der gleiche Algorithmus und die gleichen Schlüsselpaare wie in den Schritten b) bis e) verwendet werden, wodurch vor allem bei  
5 Chipkarten bei der Hardwareimplementation eine platzsparende Umsetzung ermöglicht wird. Andererseits werden hier keine originären Daten vom Prover an den Verifier übermittelt, so daß sich diese Ausführungsform besonders vorteilhaft für die Einheitenauthentikation eignet. Der Schritt a) wird in dieser  
10 Ausführungform an beliebiger Schrittposition vor Schritt f)  
ausgeführt.

Wie in einer weiteren Ausführungsform beschrieben ist, kann der Authentikationsprüfalgorithmus AUTVER dem gleichen Algorithmus entsprechen wie das vorher angewandte Verfahren AUT-  
15 GEN. Die eigentliche Authentikationsprüfung wird dann vom Verifier in ähnlicher Weise wie bei der Authentikatorerzeugung AUTGEN durch Anwendung dieses Authentikationsalgorithms auf den Datensatz im Klartext mit dem wenigstens einen Datenelement als Schlüssel durchgeführt: das Ergebnis ist gleich dem vom Prover zugesandten Authentikator, nur wenn dieser offensichtlich Besitzer des zum ersten asymmetrischen Verschlüsselungsverfahren gehörigen privaten Schlüssels ist. In diesem Fall akzeptiert der Verifier die Nachricht als vom Prover  
20 übermittelt.  
25

In einer weiteren Ausführungsform wird der Authentikationsalgorithmus aus Schritt h) als zweites Entschlüsselungsverfahren ausgebildet, welches mit dem zweiten Verschlüsselungsverfahren verschlüsselte Nachrichten entschlüsseln kann. Unter  
30 Verwendung des als Schlüssel dienenden, wenigstens einen Da-

tenelementes kann der Verifier den Authentikator entschlüsseln und erhält damit einen Datensatz, welcher mit dem ursprünglich im Klartext übermittelten Datensatz verglichen werden kann.

5

Wie in einer weiteren Ausführungsform vorgesehen ist, können in dem Fall, daß mehrere Datenelemente übertragen und zur zweiten Verschlüsselung in Schritt f) beim Prover herangezogen werden, die Schritte b) bis e) für ein einzelnes Datenelement auch blockweise ausgeführt werden, nach deren Ausführung die gleichen Schritte wieder für das nächste Datenelement ausgeführt werden etc. Dies entspricht dann einer Wiederholung der Schritte b) bis e) mit der Häufigkeit der benutzten Datenelemente.

10

In einer weiteren Ausbildung ist die Verwendung diskreter Exponentiation für das erste Ver- und Entschlüsselungsverfahren vorgesehen. Dieses ist besonders vorteilhaft, da es einerseits ein hohes Maß an Sicherheit ermöglicht, denn das Problem des diskreten Logarithmus kann von Angreifern - bei geeigneter Wahl der verwendeten algebraischen Basisstruktur - nur durch im Aufwand besonders stark mit der Größe des Exponenten ansteigenden Lösungstechniken behandelt werden.

15

Gleichzeitig wird nur wenig Speicherplatz auf z.B. einer Chipkarte benötigt.

20

In weiteren Ausbildungen sind besonders vorteilhaft ausgeführte Algorithmen für die Ver- und Entschlüsselungsverfahren sowie die Authentikatorerzeugung und -prüfung beschrieben. Dabei werden die einzelnen aufeinander abgestimmten Teilmodule über spezielle Gruppen und Halbgruppen realisiert. Hier-

durch entfällt einerseits die umständliche Langzahl-Modulo-Arithmetik, welche nach bisheriger Technik erheblichen Platzbedarf auf einem Chip erfordert, andererseits lassen sich damit die mindestens vier genannten Module bzw. Algorithmen in 5 einer gemeinsamen Basis hardwaretechnisch realisieren, welches ebenfalls Platz ggf. auf dem Chip einspart.

Weitere Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

10

Die Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand von Zeichnungen näher erläutert:

Figur 1 zeigt schematisch den Ablauf des erfindungsgemäßen 15 Verfahrens zur authentisierten Datenübertragung zwischen der beweisführenden und der verifizierenden Einheit.

Eine Chipkarte wird in den CAD (card adapter device) eines 20 Terminals gesteckt. Das Terminal erhält von der Chipkarte zu- nächst den öffentlichen Schlüssel 8 der Chipkarte versehen mit dem Zertifikat eines Trust-Centers. Die Chipkarte bzw. 25 die integrierte Schaltung auf der Chipkarte übernimmt im folgenden die Aufgabe des Provers bzw. der beweisführenden Einheit 1, da sie ihre Identität und die Authentizität ihrer Daten gegenüber dem Terminal nachzuweisen hat, welches im folgenden die Position des Verifiers bzw. der verifizierenden Einheit 2 übernimmt. Nachfolgend wird erfindungsgemäß die authentisierte Übermittlung eines Datensatzes vom Prover an den 30 Verifier beschrieben, wie in Figur 1 dargestellt ist.

Der Prover hält außerdem einen nur ihm bekannten privaten Schlüssel 7, welcher mit dem öffentlichen Schlüssel 8 ein Paar bildet. Der Verifier besitzt ein erstes Verschlüsselungsverfahren 3, mit dem die als Zufallselemente erzeugten 5 Datenelemente 9 zu einem Chiffrat bzw. verschlüsselten Datenelement 9' verschlüsselt werden können. In das Verschlüsselungsverfahren gehen desweiteren Halbgruppenelemente und zusätzlich vom Verifier erzeugte Zufallszahlen für die diskrete Exponentiation ein. Für dieses erste Verschlüsselungs- 10 verfahren 3 sowie für die weiteren noch zu beschreibenden Algorithmen werden in diesem Ausführungsbeispiel basierend auf Gruppen und Halbgruppen folgende Ausprägungen genutzt, wobei sämtliche Verknüpfungen der vorkommenden Objekte auf 15 die Arithmetik in endlichen Körpern  $GF(2^n)$  zurückführbar sind:

H : eine von dem Punkt h erzeugte Gruppe von Punkten auf einer elliptischen Kurve über  $GF(2^n)$ , wobei insbesondere H eine Halbgruppe ist;

f : ist die identische Abbildung;

20 d = k<sub>priv</sub> ist der private Schlüssel 7;

k<sub>pub</sub> = h<sup>d</sup> ist der öffentliche Schlüssel 8;

G : ist die multiplikative Gruppe in  $GF(2^n)$ ;

G<sub>1</sub> : ist die multiplikative Gruppe in  $GF(2^m)$ , mit

$$m = \frac{n - 1}{2}, \quad n \text{ ungerade}$$

25 G<sub>2</sub> : ist die additive Gruppe in  $GF(2^m)$ ;

$\pi : H \rightarrow G$  ist eine Funktion, welche einen Kurvenpunkt  $(p_x, p_y)$  der elliptischen Kurve mit  $p_x \neq 0$  auf das Element  $p_x^{-1}$  abbildet.

$\pi_1 : G \rightarrow G_1$        $\pi_1(z)$  besteht aus den oberen  $m$  Bits von  $z$

5     $\pi_2 : G \rightarrow G_2$        $\pi_2(z)$  besteht aus den unteren  $m$  Bits von  $z$

Der Protokollablauf sieht folgendermaßen aus:

Step 1 (Schritt b): der Verifier 2 erzeugt eine Zufallszahl  $t$  und ein Zufallselement  $z_1 \in G$  als Datenelement 9;

10 Step 2 (Schritt c):

i) der Verifier 2 berechnet im ersten Verschlüsselungsverfahren 3 die Elemente  $h^t$  und

$$k_{\text{pub}}^t = r = (r_x, r_y) \in H;$$

ii) der Verifier 2 berechnet im ersten Verschlüsselungsverfahren 3 aus dem öffentlichen Schlüssel 8 von  $k_{\text{pub}}$  das Element  $\pi(k_{\text{pub}}^t) = r_x^{-1} \in G$ ;

15 iii) der Verifier 2 verschlüsselt das Datenelement 9 im ersten Verschlüsselungsverfahren 3 durch die Verknüpfung  $z_1 \circ r_x^{-1} \in G$ ;

20 Step 3 (Schritt d): der Verifier 2 übermittelt als Chiffrat das verschlüsselte Datenelement 9' und das Element  $h^t$ ;

Step 4 (Schritt e):

25 i) der Prover 1 berechnet anhand des gesendeten Elements  $h^t$  im ersten Entschlüsselungsverfahren 7 mittels des privaten Schlüssels 7 durch

$(h^t)^d = (h^d)^t = k_{\text{pub}}^t = (r_x, r_y)$  den Kurvenpunkt, ohne selbst in Kenntnis von  $t$  zu sein;

ii) der Prover 1 berechnet anhand des verschlüsselten Datenelementes  $9'$  und dem berechneten Element  $r_x$  aus dem gesendeten Chiffrat im ersten Entschlüsselungsverfahren 4 mit  $z_1 = (z_1 \circ r_x^{-1}) \circ r_x \in G$  das unverschlüsselte Datenelement  $9$ ;

5

Step 5 (Schritt a): der in Figur 1 auch mit  $m$  bezeichnete Datensatz 10 wird im Klartext vom Prover 1 an den Verifier 2 gesendet;

10

Step 6 (Schritt f): der Prover 1 bildet den in Figur 1 auch mit  $D$  bezeichneten Authentikator 11 im zweiten Verschlüsselungsverfahren 5 durch die Verknüpfung

$D = \pi_1(z_1) \circ m + \pi_2(z_1)$  anhand der nun als Schlüssel verwendeten Datenelemente  $9$ ;

15

Step 7 (Schritt g): der Prover 1 übermittelt den Authentikator 11 an den Verifier 2;

20

Step 8 (Schritt h): der Verifier 2 berechnet im Authentikationsalgorithmus 6 aus der Verknüpfung  $D' = \pi_1(z_1) \circ m + \pi_2(z_1)$  den Referenzauthentikator  $11'$ , wobei der Authentikationsalgorithmus 6 die gleichen Rechenoperationen wie das zweite kryptographische Verfahren ausführt;

25

Step 9 (Schritt i): der Verifier 2 überprüft die Identität des Authentikators 11 mit dem Referenzauthentikator  $11'$ : falls  $D=D'$ , wird der Datensatz 10 mit Wert  $m$  als vom Prover 1 übermittelt akzeptiert;

Patentansprüche

1. Verfahren zur Authentikation eines Datensatzes (10) zwischen einer beweisführenden Einheit (1) und einer verifizierenden Einheit (2) in der Datenverarbeitung, umfassend die Schritte:
- a) der Datensatz (10) wird von einer der beiden Einheiten (1, 2) zur jeweils anderen derart übermittelt, daß er nach der Übermittlung beiden Einheiten (1, 2) unverschlüsselt vorliegt,
  - b) die verifizierende Einheit (2) erzeugt wenigstens ein Datenelement (9),
  - c) die verifizierende Einheit (2) verschlüsselt das wenigstens eine Datenelement (9) in einem ersten kryptographischen Verschlüsselungsverfahren (3) mittels eines der verifizierenden Einheit (2) bekannten öffentlichen Schlüssels (8) der beweisführenden Einheit (1),
  - d) die verifizierende Einheit (2) übermittelt das wenigstens eine verschlüsselte Datenelement (9') an die beweisführende Einheit (1),
  - e) die beweisführende Einheit (1) entschlüsselt das wenigstens eine verschlüsselte Datenelement (9') in einem dem ersten Verschlüsselungsverfahren (3) zugeordneten ersten Entschlüsselungsverfahren (4) mittels eines nur ihr bekannten privaten Schlüssels (7),
  - f) die beweisführende Einheit (1) berechnet aus dem zu authentisierenden Datensatz (10) in einem zweiten kryptographischen Verfahren (5) einen von dem wenigstens einen Datenelement (9) abhängigen Authentikator (11),
  - g) die beweisführende Einheit (1) übermittelt den Authentikator (11) an die verifizierende Einheit (2),

- h) die verifizierende Einheit (2) prüft mit Hilfe eines dem zweiten kryptographischen Verfahren (5) zugeordneten Authentikationsprüfalgorithmus (6) unter Verwendung des wenigstens einen unverschlüsselten Datenelementes (9) und des Datensatzes (10) den Authentikator (11),  
5 i) in Abhängigkeit vom Prüfergebnis akzeptiert die verifizierende Einheit (2) den Datensatz (10) als von der beweisführenden (1) Einheit übermittelt.

10 2. Verfahren nach Anspruch 1,

d a d u r c h g e k e n n z e i c h n e t , d a ß  
in Schritt a) die beweisführende Einheit (1) den Datensatz (10) unverschlüsselt an die verifizierende Einheit (2) übermittelt.

15

3. Verfahren nach Anspruch 1,

d a d u r c h g e k e n n z e i c h n e t , d a ß  
die verifizierende Einheit (2) den Datensatz (10) als Zufallselement erzeugt und anschließend in Schritt a) den Datensatz 20 (10) an die beweisführende Einheit (1) übermittelt.

4. Verfahren nach einem der Ansprüche 1 bis 3,

d a d u r c h g e k e n n z e i c h n e t , d a ß  
in Schritt h)

25 - der Authentikationsprüfalgorithmus (6) im wesentlichen identisch mit dem zweiten kryptographischen Verfahren zur Authentikatorerzeugung (5) ist,  
- der Authentikationsprüfalgorithmus (6) von der verifizierenden Einheit (2) auf das wenigstens eine unverschlüsselte 30 Datenelement (9) und den Datensatz (10) zur Bildung eines Referenzauthentikators (11') angewendet wird,

- der Referenzauthentikator (11') mit dem Authentikator (11) verglichen wird.

5. Verfahren nach einem der Ansprüche 1 bis 3,

5 dadurch gekennzeichnet, daß  
in Schritt h)

- der Authentikationsprüfalgorithmus (6) aus einem Entschlüsselungsverfahren besteht, das dem zweiten kryptographischen Verfahren (5) zur Erzeugung eines Authentikators, dem zugehörigen Verschlüsselungsverfahren, entspricht,
- der Authentikationsprüfalgorithmus (6) von der verifizierenden Einheit (2) auf den Authentikator (11) durch Entschlüsselung zur Bildung eines Referenzdatenelementes und eines Referenzdatensatzes angewendet wird,
- das Referenzdatenelement und der Referenzdatensatz mit dem unverschlüsselten Datenelement (9) und dem unverschlüsselten Datensatz (10) verglichen werden.

6. Verfahren nach einem der Ansprüche 1 bis 5,

20 dadurch gekennzeichnet, daß

- die Schritte b), c), d) und e) zur Erzeugung wenigstens eines weiteren Datenelementes (9) vor Schritt f) wiederholt werden,
- die beweisführende Einheit (1) den zu authentisierenden Datensatz (10) in Schritt f) in Abhängigkeit von dem wenigstens einen Datenelement (9) und dem wenigstens einen weiteren Datenelement (9) zu einem Authentikator (11) verschlüsselt.

30 7. Verfahren nach einem der Ansprüche 1 bis 6,

dadurch gekennzeichnet, daß

das erste kryptographische Verschlüsselungsverfahren (3) und das diesem zugeordnete erste Entschlüsselungsverfahren (4) mittels diskreter Exponentiation in einer Halbgruppe durchgeführt wird.

5

8. Verfahren nach Anspruch 7,  
dadurch gekennzeichnet, daß das erste kryptographische Verschlüsselungsverfahren (3) und das diesem zugeordnete erste Entschlüsselungsverfahren (4)  
10 mittels eines Algorithmus basierend auf elliptischen Kurven durchgeführt wird.

9. Verfahren nach einem der Ansprüche 7 oder 8,  
dadurch gekennzeichnet, daß  
15 das erste kryptographische Verschlüsselungsverfahren (3) die folgenden Operationen umfaßt:

- die verifizierende Einheit (2) erzeugt eine Zahl  $t \in T$ , wobei  $T$  ein Teilbereich der ganzen Zahlen ist,
- die verifizierende Einheit (2) berechnet das Element  
20  $h^{f(t)} \in H$ , wobei  $f : T \rightarrow T'$  eine Abbildung in einen nicht notwendigerweise von  $T$  verschiedenen Teilbereich  $T'$  der ganzen Zahlen ist,  $H$  eine durch das Element  $h$  erzeugte, multiplikativ geschriebene Halbgruppe darstellt mit der diskreten Exponentiation zur Basis  $h$  als Einwegfunktion in  
25 der Halbgruppe  $H$ ,
- die verifizierende Einheit (2) berechnet aus dem öffentlichen Schlüssel (8),  $k_{\text{pub}} = h^{f(d)} \in H$ , das Element  
 $\pi(k_{\text{pub}}^{f(t)}) \in G$ , wobei  $\pi : H \rightarrow G$  eine Abbildung der Halbgruppe  $H$  in eine Gruppe  $G$  angibt,  $d = k_{\text{priv}} \in T$  der nur  
30 der beweisführenden Einheit zugängliche private Schlüssel

(7) ist, und die Abbildung  $t \rightarrow h^{f(t)} \rightarrow \pi(h^{f(t)})$  vom Teilbereich der ganzen Zahlen  $T$  auf die Gruppe  $G$  eine Einwegfunktion darstellt,

- die verifizierende Einheit (2) verschlüsselt das wenigstens  
5 eine Datenelement (9),  $z$ , durch eine Verknüpfung zum ver-  
schlüsselten Datenelement (9'),  $z' = z \circ \pi(k_{pub}^{f(t)}) \in G$ .

10. Verfahren nach Anspruch 9,

d a d u r c h g e k e n n z e i c h n e t , d a ß

10 die verifizierende Einheit (2) in Schritt d) zusätzlich zum verschlüsselten Datenelement (9') das Element  $h^{f(t)} \in H$  an die beweisführende Einheit (1) übermittelt.

11. Verfahren nach Anspruch 10,

15 d a d u r c h g e k e n n z e i c h n e t , d a ß  
das erste kryptographische Entschlüsselungsverfahren (4) die folgenden Operationen umfaßt:

- die beweisführende Einheit (1) berechnet mittels der Funktion  $f$ , des Elementes  $h^{f(t)} \in H$  und des nur ihr bekannten privaten Schlüssels  $d$  das Element  $k_{pub}^{f(t)} \in H$ ,

- die beweisführende Einheit (1) berechnet das zum Element  $\pi(k_{pub}^{f(t)}) \in G$  inverse Element  $\pi'(k_{pub}^{f(t)}) \in G$ ,

- die beweisführende Einheit (1) entschlüsselt das verschlüsselte Datenelement (9') durch die Verknüpfung des verschlüsselten Datenelementes mit dem inversen Element:

$$z = z' \circ \pi'(k_{pub}^{f(t)}),$$

wobei dem ersten kryptographischen Entschlüsselungsverfahren (4) die gleichen Abbildungen  $f$ ,  $\pi$  und die gleiche Verknüpfung

- zugrundeliegen wie dem ersten kryptographischen Verschlüsselungsverfahren (3).

12. Verfahren nach Anspruch 11,

5 dadurch gekennzeichnet, daß das zweite kryptographische Verfahren (5) die folgenden Operationen umfaßt:

- die beweisführende Einheit (1) berechnet aus dem wenigstens einen unverschlüsselten Datenelement  $z$  ein Element

10  $g_2 = \pi_1(z) \in G_1$  und ein Element  $g_2 = \pi_2(z) \in G_2$ , wobei  $G_1$  und  $G_2$  Gruppen mit  $G_1 \subset G_2$  darstellen und  $\pi_1 : G \rightarrow G_1$  und  $\pi_2 : G \rightarrow G_2$  Funktionen darstellen, welche Elemente der Gruppe  $G$  auf die Gruppen  $G_1$  oder  $G_2$  abbilden,

15 - die beweisführende Einheit (1) transformiert den zu authentisierenden Datensatz (10),  $m$ , zu einem Element  $g' = (g_1 * m)$  mit einer Gruppenverknüpfung  $*$  in  $G_1$ ,

- die beweisführende Einheit (1) berechnet den Authentikator (11),  $D$ , durch  $D = \text{inj}(g') \bullet g_2$  mit der Gruppenverknüpfung  $\bullet$  in  $G_2$ , wobei die Abbildung  $\text{inj} : G_1 \rightarrow G_2$  Elemente aus  $G_1$

20 injektiv in  $G_2$  abbildet.

13. Verfahren nach einem der Ansprüche 1 bis 12,

dadurch gekennzeichnet, daß vor Schritt b)

25 - die beweisführende Einheit (1) ihren öffentlichen Schlüssel (8) mit einem Zertifikat eines Trust-Centers übermittelt,  
- die verifizierende Einheit (2) mittels eines Zertifizierungsverfahrens die Gültigkeit des öffentlichen Schlüssels (8) der beweisführenden Einheit (1) überprüft,

- die verifizierende Einheit (2) die Kommunikation mit der beweisführenden Einheit (1) in Abhängigkeit des Ergebnisses der Überprüfung fortsetzt.

5 14. Verfahren nach einem der Ansprüche 1 bis 13,  
dadurch gekennzeichnet, daß  
die beweisführende Einheit (1) eine integrierte Schaltung auf  
einer Chipkarte ist, und die verifizierende Einheit (2) ein  
Chipkartenterminal ist.

10

15. Verfahren nach einem der Ansprüche 1 bis 13,  
dadurch gekennzeichnet, daß  
die beweisführende Einheit (1) eine integrierte Schaltung in  
einem Identifikations-/Authentikationstoken ist, welches fest  
15 mit einem nicht ortsbundenen Objekt verbunden ist.

20 16. Verfahren nach einem der Ansprüche 14 oder 15,  
dadurch gekennzeichnet, daß  
die Kommunikation zwischen beweisführender Einheit (1) und  
verifizierender Einheit (2) kontaktlos erfolgt.

Zusammenfassung

Verfahren zur Authentikation

- 5 Eine Methode zur Authentikation und Identifikation verwendet einerseits unterschiedliche Schlüssel (7, 8) für den Prover (1) und den Verifier (2), verzichtet andererseits aber auf die Benutzung von Langzahl-Modulo-Arithmetik durch die Verwendung einfacher Grundkomponenten wie beispielsweise arithmetische Operationen in endlichen Körpern  $GF(2^n)$ . Ein  
10 privater Schlüssel (7) ist beim Prover (1) hinterlegt, so daß dieser als Zufallselemente erzeugte Datenelemente (9) verschlüsselt empfangen und selber wieder als Schlüssel für ein  
Authentikationsverfahren eines zu übertragenden Datensatzes  
15 10 benutzen kann. Der Verifier (2) empfängt den so gebildeten Authentikator (11) und prüft ihn. Wird der Datensatz vom Verifier (2) erzeugt und an den Prover (1) gesendet, so kann dieses Verfahren zur Identifikation des Provers (1) dienen.  
Besonders vorteilhaft ist diese Verfahren im Bereich von  
20 Chipkarten, da dort der benötigte Platz bei der Hardwareimplementation erheblich reduziert werden kann.

Figur 1

Bezugszeichenliste

- 1 Beweisführende Einheit, Prover
- 2 Verifizierende Einheit, Verifier
- 5 3 erstes Verschlüsselungsverfahren, asymmetrisch
- 4 erstes Entschlüsselungsverfahren, asymmetrisch
- 5 zweites kryptographisches Verfahren; Algorithmus zur  
Erzeugung eines Authentikators
- 6 Authentikationsprüfalgorithmus
- 10 7 privater Schlüssel
- 8 öffentlicher Schlüssel
- 9 Datenelement, unverschlüsselt
- 9' Datenelement, verschlüsselt
- 10 Datensatz
- 15 11 Authentikator
- 11' Referenzauthentikator

Fig 1

